UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/215,058	12/17/1998	NED HOFFMAN	STA-14	7856

7590 05/16/2005

MARGER JOHNSON & MCCOLLON, P.C.
1030 S. W. MORRISON STREET
PORTLAND, OR 97205

EXAMINER	
MYHRE, JAMES W	
ART UNIT	PAPER NUMBER
3622	

DATE MAILED: 05/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/215,058
Filing Date: December 17, 1998
Appellant(s): HOFFMAN ET AL.

Ariel S. Rogson
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed February 22, 2005.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

6,070,141	HOUVENER et al	5-2000
5,291,560	DAUGMAN	3-1994

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

(a) Claims 1-12 and 23-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Houvener et al (6,070,141) in view of Daugman (5,291,560) .

Claims 1, 2, 23, 24, 27, 29, and 30: Houvener discloses a method for authorizing transactions using biometric identification, comprising:

a. Registering the user's (customer's) biometric and account data (col 11, lines 33-37);

b. Transmitting at least a biometric sample to a remote authentication system (col 7, line 45 - col 8, line 6);

c. Comparing the transmitted biometric data with the stored registered biometric data to verify the identity of the customer (col 9, lines 16-21 and col 10, lines 8-15);

d. Transferring the payment between the customer's account and the merchant's account (or another of the user's accounts, e.g. electronic funds transfer from checking account to savings account) once it has been determined that the customer's account has sufficient funds (within its pre-approval credit limit)(col 7, line 45 - col 8, line 6); and

e. Presenting the results to the customer, merchant, or both (optional)(col 8, lines 3-6).

Houvener discloses that a first of at least two identification units is input to the system by the customer ("person to be identified") at the point of sale, then transmitted to the database, which uses the first identification unit to locate a stored second identification information unit that is mapped to the received first identification information unit. Houvener also discloses that the first identification information unit is any form of identification such as a driver's license number, a social security number or the like (col 9, lines 36-39) and that the second identification information unit is preferably biometric data pertaining to the customer. The system will then compare the stored biometric data with a biometric data sample supplied by the customer at the POS. Since the account number and the biometric data are linked within the database it would have been obvious to one having ordinary skill in the art at the time the invention was made once the identity of the customer has been verified that in order to approve the transaction needs to be approved as discussed by Houvener. This approval in Houvener takes place through the normal credit card or banking approval channels using the account number that is linked to the identified individual. As Houvener claims in Claim 21, either of the identification information units could comprise a biometric identifier; thus, implying that the first identification information unit above could be the biometric identifier, not the account number. Thus, the biometric identifier could be used as the input to find the other part of the linked data, the account number. Moreover, the use of biometric data by Houvener to actually identify the individual (and, thus, his account) eliminates the need to use the account number to identify the individual, especially when combined with Daugman (see below).

While Houvener discloses comparing the customer's current biometric data with the stored biometric data to verify the identity of the customer (i.e. a one-to-one comparison) and that the database contains identification information about a plurality of persons (col 11, lines 33-38), it is not explicitly disclosed that the current biometric data is being compared to biometric samples from the plurality of customers in the database (i.e. a one-to-many) to determine the identity of the current customer. Daugman discloses a similar method for using biometric data (iris codes) to identify individuals in which the comparison may be between "two iris codes, as well as exhaustive searches through large databases of stored iris codes" and "could exhaustively compare a 'presenting' iris code against a population of 80 million previously stored iris codes within one second, to establish reliably whether the individual is any one of those persons" (col 18, lines 1-9). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to compare the current biometric data collected by Houvener against the plurality of stored biometric data to identify the customer and, since Houvener has linked the customer's account and biometric data, the customer's account number. One would have been motivated to compare the current biometric data to a plurality of stored biometric data in order to automatically and unobtrusively identify the customer without the need for the customer to present any kind of token, PIN number, signature, or the like automatically as discussed by Daugman (col 1, lines 52-55).

While Houvener discloses using this biometric identification system for electronic transactions and banking functions to include transferring funds between accounts and explicitly discloses that the store clerk will be positively identified by the use of a smart card and PIN so that "the system can recreate a transaction and identify not only the person initiating the transaction but the clerk who was responsible for positively identifying the individual initiated the transaction" (col 11, lines 6-9), it is not explicitly disclosed that the merchant's account is going to be pre-registered with the system, nor that the merchant proposes a transaction offer to the customer. The Examiner notes that it is common to pre-register merchants and their account numbers with commerce systems for a variety of reasons. For example, pre-registering merchants provides a higher level of assurance to the customer that the merchant is an "approved" merchant that can be trusted to provide the goods/services. Pre-registering merchants also enabled the system to charge a pre-negotiated transaction fee to the merchant, such as is common with credit card transactions. By pre-registering, merchants are also able to complete transactions without having to transmit their account number over unsecure lines (e.g. the Internet) each time. For these and other well known benefits, it would have been obvious to one having ordinary skill in the art at the time the invention was made to register the merchant and to include at least one of the merchant's financial account number. One would have been motivated to include such a registration step for the merchants in the Houvener invention in view of the reasons above and Houvener's discussion of the importance of data protection on the Internet and processing the credit card transaction.

The Examiner notes that the definition of the merchant's transaction offer in Claim 1, wherein "the proposed commercial transaction comprising price information", reads on a catalogue, an advertisement, sales flyer, or verbal price quote by the merchant. Since almost all customers (except, possibly, extremely rich customers) would want to know the price of the goods/services before purchasing the goods/services, it would have been obvious to one having ordinary skill in the art at the time the invention was made for the merchant to present the price of the goods/services to the customer. One would have been motivated to present the price to the customer in order to allow the customer to make a better business decision on the quality of the offer.

Claims 3-6 and 31: Houvener and Daugman disclose a method for authorizing transactions using biometric identification as in Claims 28 and 29 above, neither reference explicitly discloses using an account code to select an account, assigning a name to the account code, nor displaying a list of the accounts to the customer upon successful identification. Official Notice is taken that it is old and well known within the banking arts to display a list of accounts to a user (such as when operating an ATM terminal) and to identify the accounts using account codes and account names. For example, when a customer logs onto an ATM terminal and selects the type of desired transaction, the terminal will display a list of pertinent accounts and ask the customer to select one or more (depending upon the type of transaction). The list of accounts do not normally show the entire account number, which may be quite extensive in length, but rather the list consists of an account code (e.g. A, B, C, and D) and an associated

account name (e.g. checking, savings, Christmas Club, money market). The customer normally selects the desired account by pressing the keyboard button indicated by the account code. A similar system is used to allow a customer to select the desired account when completing a transaction at a merchant's facility, such as a travel agency. If the customer has several travel accounts (e.g. business, executive, and personal), the system will display the list of the customer and allow the customer to enter the account code for the desired travel account. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to display a list of accounts to Houvener customer using account codes and account names and to allow the customer to select the desired account. One would have been motivated to display and use such a list in order to eliminate the need for the customer to remember the lengthy account numbers of each account, thus facilitating a more expeditious selection of the desired account and decreasing the opportunity for erroneous (undesired) selections.

Claim 7: Houvener and Daugman disclose a method for authorizing transactions using biometric identification as in Claim 1 above, but neither reference explicitly discloses creating a credit authorization draft. The Examiner takes Official Notice that credit authorization drafts as disclosed by Claim 7 were well known within the business arts and have been used extensively in business-to-business transactions to allow transactions to be completed, for example, without the need to pre-approve a transaction in which the final price may not be known ahead of time (e.g. repair of an office machine). Therefore, it would have been obvious to one having ordinary skill in

the art at the time the invention was made to create a credit authorization draft in the Houvener reference. One would have been motivated to include the creation of a credit authorization draft in the Houvener reference in order to facilitate business-to-business transactions without overburdening the two accounting departments.

Claim 8: Houvener and Daugman disclose a method for authorizing transactions using biometric identification as in Claim 2 above, and Houvener further discloses the data being communicated between remote computer systems to determine resources and/or construct the credit authorization draft (col 7, line 45 - col 8, line 6).

Claim 9: Houvener and Daugman disclose a method for authorizing transactions using biometric identification as in Claim 1 above. While Houvener discloses including and storing the transaction data as a transaction record, it is not explicitly disclosed that the transaction data contains one or more of a list of goods/services, a seller name, a date and time, a location, or an invoice number. The Examiner notes that these are well known elements usually contained in transaction data files. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include one or more of these elements in the Houvener transaction data. One would have been motivated to include these features in order to facilitate delivery of the purchased goods/services and to better identify the transaction for accounting processing by all parties concerned, especially when attempting to "recreate a transaction" as discussed by Houvener (col 11, lines 4-9).

Claim 10: Houvener and Daugman disclose a method for authorizing transactions using biometric identification as in Claim 28 above, but neither reference explicitly discloses that the customer can receive cash back during the transaction. The Examiner takes Official Notice that cash back transactions were extremely well known throughout society at the time the invention was made and have been the major means for many people to maintain their supply of cash-on-hand for small purchases. For support of this notice, the Examiner is forwarding a patent (Patent Re 30,821) issued to Goldman in 1981 which extensively discusses cash back transactions at a point of sale terminal in which the system uses the symbol "CB" to indicate a cash back transaction or the signal "NC" to indicate a no-cash transaction. (col 8, lines 32-33). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to allow the customer in Houvener to receive cash back during a transaction by entering an amount that exceeds the amount of the goods/services being purchased. One would have been motivated to allow a cash back transaction in order to increase customer satisfaction and goodwill and to allow the customer to have the cash to "tip" the merchant representative for exceptional service, provide change for parking meters, etc.

Claim 11: Houvener and Daugman disclose a method for authorizing transactions using biometric identification as in Claim 1 above. Houvener further discloses checking incoming registration biometric samples against previously stored biometric samples to prevent duplicate registration of individuals, either inadvertently or for fraudulent purposes (col 6, lines 52-67 and col 7, lines 38-42).

Claim 12: Houvener and Daugman disclose a method for authorizing transactions using biometric identification as in Claim 1 above. Houvener further discloses the type of biometric data being used consisting of one or more of "fingerprints, retinal images, or the like" (col 9, lines 16-20).

Claims 25 and 26: Houvener and Daugman disclose a method for authorizing transactions using biometric identification as in Claim 1 above. Houvener further discloses that the merchant will be identified by comparing stored identification data with identification data received over the remote connection. As an example, Houvener suggests the use of "commonly available caller ID technology to ensure that the request for data has originated from an authorized telephone line" (col 6, lines 20-31). Since Houvener also discloses that the system could be run not only through telephone network (hence, the caller ID example), but also through a wide area network, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use other known technology for verifying the sending unit in Houvener, to include network address comparison, hardware identification number comparison, etc. One would have been motivated to use the hardware identification code in the identification comparison in view of its uniqueness, since manufacturers do not give the same hardware identification number to two items.

Claim 28: Houvener and Daugman disclose a method for authorizing transactions using biometric identification as in Claim 1 above, and Houvener further discloses adding the customer's current biometric data to the transaction offer data upon acceptance of the transaction by the customer (col 7, line 45 – col 8, line 6).

(11) Response to Argument

(a) The Appellant argues that "Houvener discloses using a biometric sample to verify an already-made identification, not to make a primary identification" and uses a two-step process for verifying the identity of an individual, whereas the present invention uses a one-step process (pages 5-8). The Appellant continues by arguing that the Examiner's interpretation of Houvener's Claim 21 is not enabled and would require the account number be used to verify the user's identity. However, Claim 21's parent claim, Claim 20, discloses receiving a first identification unit from the user and transferring (and displaying) a second identification unit back to the terminal (e.g. cash register). Claim 21 adds that *at least one* of the two identification units comprises a biometric identifier. This encompasses three possibilities. First, the first identification unit may be a biometric identifier and the second identification unit is not a biometric identifier. Second, the first identification unit is not a biometric identifier and the second identifier is a biometric identifier. And third, both the first and the second identification units are biometric identifiers. In both the first and third possibilities, the biometric identifier is used to initially identify the user, as in the claimed invention. In the third possibility, the second identification unit is also a biometric identifier, which is used by the sales clerk to verify the identity of the user. For example, the user may enter a fingerprint (a biometric identifier) as the first identification unit. The system would transmit the fingerprint to be compared against the fingerprints on file in order to identify the user. Once the user has been identified, the system returns another biometric identifier, such as a photographic

image (see Houvener's Claim 22), to the terminal for use by the sales clerk in verifying the identity of the user. Since the user in Houvener has pre-registered not only his biometric identifier(s) with the system, but also his account number(s), the system has already completed the Appellant's invention of using the biometric identifier to identify the user and the user's account. The addition of a step for the sales clerk to verify the user's identity using a second biometric identifier is a superfluous, but obvious, extension which adds a further level of security to Houvener's invention and could also be appended to the Appellant's invention to provide the same additional level of security. Thus, Houvener uses a one-step process to initially identify the user, and then uses another one-step process to verify the identity.

(b) The Appellant argues that "Daugman teaches only iris identification and does not disclose nor enable the use of iris identification to complete a commercial transaction" (page 8). The Examiner notes that, as has been previously discussed in the prior Office Actions, Daugman explicitly discloses the reason for requiring such reliable identification of the individual is that "human activities and transactions have proliferated in which rapid and reliable personal identification is required. Examples include passport control, computer login control, bank automatic teller machine and *other transaction authorizations*, premises access control, and security systems generally" (emphasis added)(col 1, lines 10-17). Therefore, Daugman does discuss using his one-step process for identifying an individual for authorization of a (commercial) transaction.

(c) The Appellant argues in reference to Claims 3-6 and 31 that neither reference shows "a user assigning an index code to each of the user accounts at the registration step" (page 9). The Examiner notes that in Claim 3 the index code that the user assigns to an account "comprises one or more alphanumeric characters", i.e. a name such as 'savings', 'checking', 'Christmas fund', etc. In the rejection of these claims Official Notice was taken that it was old and well known to display a list of accounts to a user such as when operating an ATM terminal and to use account codes and account names to enable the user to differentiate between the accounts. The Appellant has not previously disagreed with this Official Notice and is not disagreeing with it in this Brief. Instead, the Appellant is now arguing that these account codes or account names are not selected (assigned) by the user when registering with the system, but by some third party. However, the Examiner notes that it is also old and well known to allow users (e.g. bank customers) to select names for their accounts. For example, when setting up three education savings accounts for his three children, a user may name them "Education Account 1", "Education Account 2", and "Education Account 3" or else "Education Account – Jim", "Education Account – John", and "Education Account – Joe". If the user did not assign unique names (codes) to these accounts, it would be difficult for the user to identify a specific one of the accounts when making a deposit or withdrawal. Since all three accounts are of the same type, the account numbers assigned by the bank would all start with the same series of alphanumeric characters to identify them as education savings accounts, only the last 4-6 characters would be different. Thus, the user would have to either remember which

account number was for which of his children or else look them up for each transaction. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to allow the user to assign unique codes or names to each of the accounts while registering them with the system. One would have been motivated to allow the user to assign these codes or names instead of using generic account names (e.g. "savings") in order to facilitate the user being able to remember and to quickly identify a specific account among a plurality of similar accounts.

(d) The Appellant argues in reference to Claim 11 that Houvener does not teach the same way "to recognize a user registering multiple times with the system" (page 10). Claim 11 reads that "*the user's registration biometric samples are compared against previously designated biometric samples of certain users wherein if a match occurs, the computer system is alerted to the fact that the user has re-registered, whereby users who perpetrate fraud on the system can be automatically identified from their biometrics alone if and when they re-register*". The first part of this claim, comparing the biometric sample to other pre-stored biometric samples, is the identification step of Claim 1 discussed above. The second part of the claim is using this matching identification to alert the system to fraudulent action by the user, e.g. re-registering. The Examiner assumes that the Appellant is alerting the system when a user is attempting to re-register the *same* accounts also, not just adding *new* accounts under his identity. Houvener discusses numerous ways to prevent fraud by the user and to notify the system when suspected fraudulent activity is detected (col 6, line 52 – col 7. line 44; col 8, line 42 - col 9, line 4; and col 11, lines 10-24). These methods would not only detect

when a user is attempting to re-register (the same account numbers), but would also detect other fraudulent activities, such as using the same user identifier at different sales terminals at substantially the same time when the distance between the terminals precludes the possibility of doing so.

(e) The Appellant argues in reference to Claim 29 that Houvener does not disclose that "*the user identification step is completed by the computer system after the comparison of the bid biometric with the registration biometric samples*" and in reference to Claim 30 that "*the user identification step is completed without transmitting any information from the computer system to the user or seller*" (pages 10-11). As discussed above, the user identification step in Houvener is complete after the comparison has been made and no information is sent between the computer system and the user or seller during this step. During the subsequent verification of the identity information is returned to the seller location to be used by the seller to verify the identity of the user. However, this is separate and distinct from the initial identification step and, as also discussed above, could be appended to the identification step of both Houvener and the Appellant inventions. The Examiner also further notes that Claim 29 does not say that "the identification *is complete* after the comparison" as argued by the Appellant, but says that the identification step *is completed* after the comparison. This refers to the time period during which the identification is made, i.e. *after* the comparison, not *before*. In both the Appellant's invention and in Houvener's invention, the identification step cannot be completed *before* the comparison is done, since the comparison is being performed in order to identify the user.

(f) In response to the Appellant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). As shown above, the Examiner has not used hindsight to redesign the teachings of Houvener, but has pointed out which parts of the Houvener invention correspond to the Appellant's invention. Whether or not the Houvener invention also discloses additional features, such as further verifying the identity of the user once that identity has been determined, does not detract from the fact that the initial identification of the user is accomplished using substantial the same method in both inventions.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

JWM
May 11, 2005

James W. Myhre
Primary Examiner

Conferees

Eric Stamber

Yehdega Retta

MARGER JOHNSON & MCCOLLON, P.C.
1030 S. W. MORRISON STREET
PORTLAND, OR 97205